


DEPARTMENT OF PERSONNEL & ADMINISTRATION		HIPAA Policy No.	9
		Current Effective Date	May 1, 2006
		Original Effective Date	May 1, 2006
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT		Approved by: Jeffrey C. Schutt	
DEVICE AND MEDIA CONTROLS		Date: 4/25/06	

I. Purpose

To define disposal and re-use guidelines for media and devices that contain electronic protected health information (ePHI) or through which ePHI can be accessed.

II. Policy

A. Copying and Storing ePHI

1. Employees are prohibited from copying ePHI onto diskettes, CDs, DVDs, external hard drives, memory sticks, zip drives, flash drives, or any other type of removable or reusable media.
2. Employees are prohibited from storing ePHI on diskettes, CDs, DVDs, external hard drives, memory sticks, zip drives, flash drives, or any other type of removable or reusable media.

B. Exceptions for Authorized IT Personnel

IT personnel may have a need to copy and/or store ePHI in the normal course of business. Reasons include routine backing up of data, creating a retrievable exact copy of ePHI before moving or repairing equipment, and using forensic software applications. These activities are permitted, as set forth below.

1. Data Back Up
 - a. DPA servers are routinely backed up, and data, including ePHI, are copied to backup tapes.
 - b. Tapes containing ePHI may be reused on the same server or stored off site in accordance with DPA's policies and relevant State and Federal laws, including HIPAA.
 - c. After final use, backup tapes must be sanitized or destroyed such that the ePHI cannot be recreated, and then disposed of.
2. Moving or Repairing Hardware
 - a. When moving or repairing computer hardware, it may be necessary for IT personnel to create a retrievable exact copy of ePHI before moving or repairing the equipment. ePHI may be copied only to a computer system with the same level of security as the system on which the ePHI normally resides.
 - b. When the copy is no longer needed, the IT employee must restore the data, if restoration is necessary, and delete the copied ePHI from the system onto which it was copied.

3. Forensic use

- a. Forensic use of ePHI requires authorization from DPA's Chief Information Officer (CIO) or delegate.
- b. All ePHI captured for forensic use must be deleted from the computer system or other electronic media used once there is no longer a need for the ePHI to be maintained in such a manner.
- c. Any disposable media used for forensic purposes, such as diskettes, CDs, and DVDs, must be sanitized or destroyed such that the ePHI cannot be recreated, and then disposed of, once there is no longer a need for the ePHI to be maintained in such a manner.

III. Procedures

IT procedures regarding the backing up of data, creating a retrievable exact copy of ePHI before moving or repairing hardware, and forensic use of ePHI shall be developed by the appropriate IT unit and must be approved by the CIO or delegate.

IV. Definitions/Abbreviations

None

V. Revision History

<u>Date</u>	<u>Description</u>
May 1, 2006	Original document

VI. References/Citations

<u>Security Rule</u>	
45 CFR 164.310(d)	Device and Media Controls